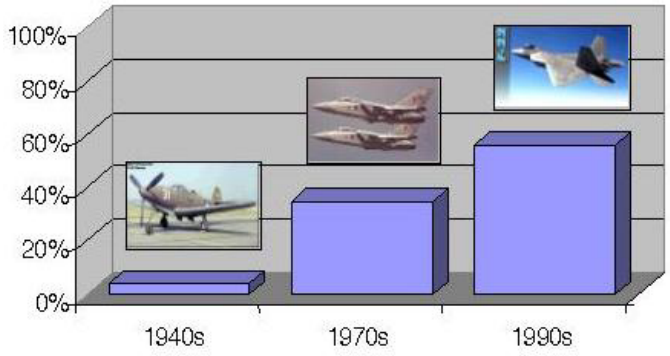
ISWHM: Tools and Techniques for Software and System Health Management

Johann Schumann, RIACS/USRA

NASA Ames

IVHM in Aircraft

- Modern aircraft
  - Have IVHM for major electrical/mechanical subsystems
    - Important for safety, reliability, environmental impact, economical considerations
  - Rely heavily on SW
    - but: mo health mgmt system for SW



Avionics costs = SW costs

Many Software problems

State-of-the-art

K.I.S.S.: Attach SW to IVHM

not that easy...

- Software problems don't develop over time
  - come in during all phase of SW life cycle
  - "don't go away"
- SW failures mostly occur instantly–HW often fails gradually (e.g., an oil leak)

HW-SW Interaction

- HW (e.g., sensors) can behave differently than expected (and thus cause a SW failure)
  - on purpose: use same SW for different HW
    - Ariane V failure
  - accidentially during development
    - DART: new GPS system just before launch
  - HW failure
    - broken cable
    - disabled sensor (e.g., Deep Space I)
  - gradual degradation
    - increase of sensor noise

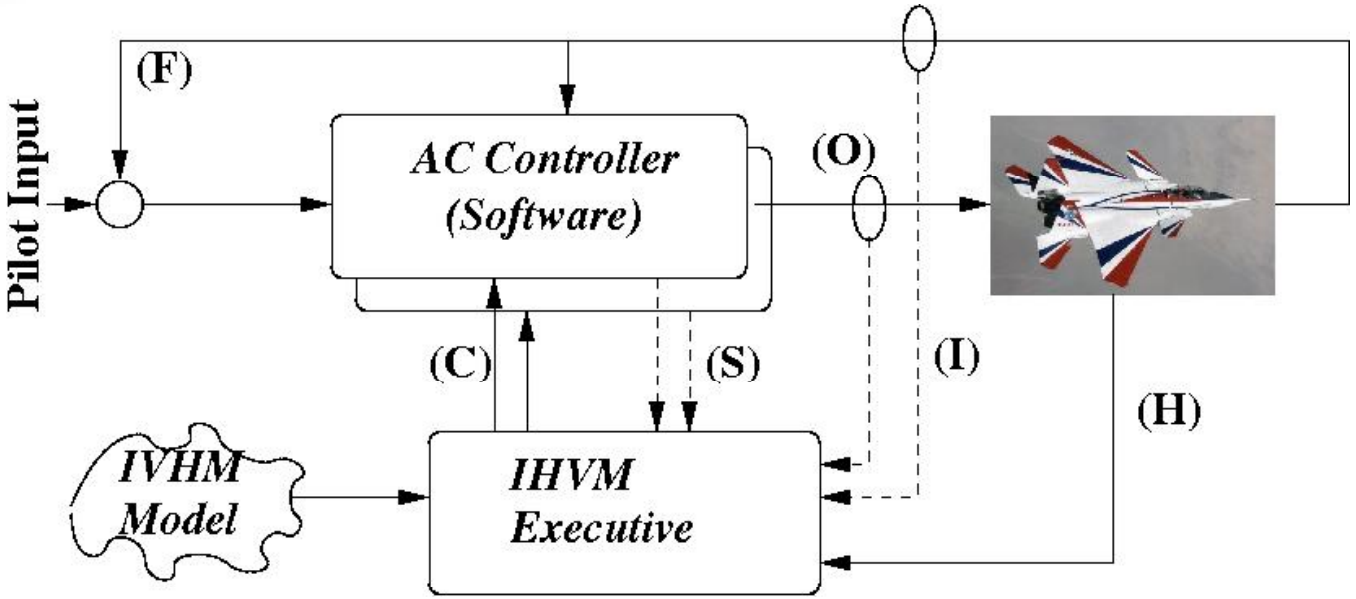
SW IVHM is SW

Quis custodiet ipsos custodes?

Juvenal

- The IVHM system that monitors the SW system must be at least reliable as the SW under scrutiny
  - false alarms are not an option
  - un-detected failures are a safety hazard
- Rigorous V&V of IVHM system necessary, state-of-art testing not sufficient

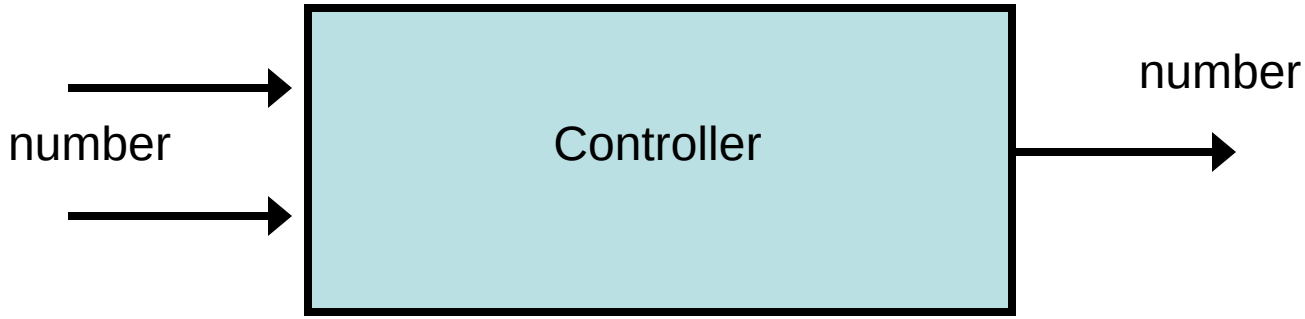
Proposed ISWHM Architecture



- Probabilistic quality metric and runtime-verification for (hybrid) controller
- Advanced (Bayesian) IVHM system
- IVHM executive/reasoner subject to V&V

Health Metric

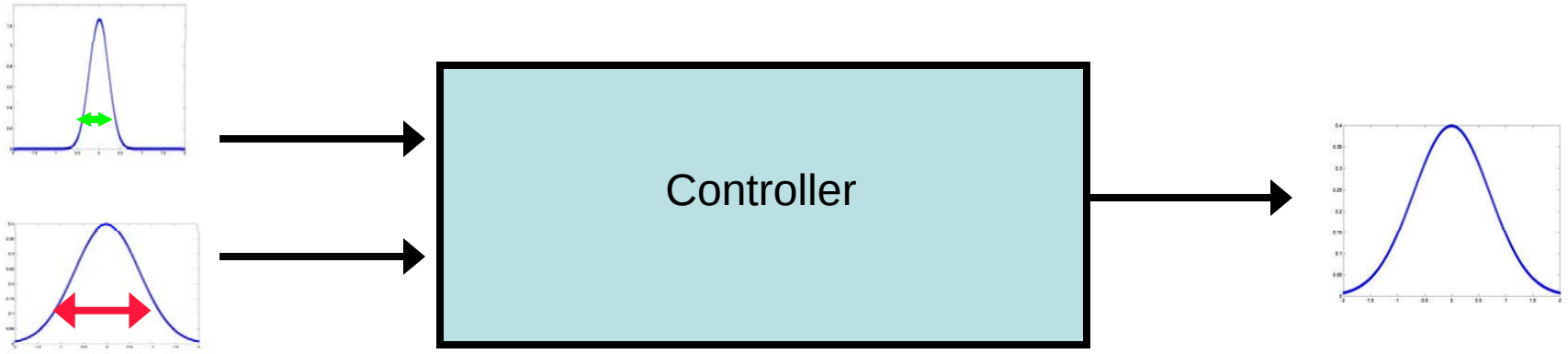
- Traditionally, an algorithm (e.g., control system) takes numerical data and produces numerical data.



The output produced doe not contain any notion of
- quality of input data (e.g, are the sensor data OK or noisy?)
- quality of calculation (big round-off errors?)
- quality of internal parameters (are we at the stability limit of the controller)?

Health Metric

- An algorithm with built-in health metric takes probability variables as inputs and outputs.
- Shape and width of the Probability density function comprises the health metric



Narrow Gauss curves = good quality/health
Wide gauss curves = bad quality/health

Conclusions

I. *Software Health Management integrated seamlessly into IVHM*

II. *Statistical Quality Metric for continuous components combined with Runtime Verification/Monitoring of discrete SW*

III. *IVHM reasoner/executive verification*

IV. *All flight-critical software must be certified: Dependability and Safety Cases*